

WHAT IS CLAIMED IS:

- 1 1. A system for managing volatile storage of information for operating a
2 device having extended periods of inactivity between periods of activity
3 comprising:
4 volatile memory connected to receive said information from a
5 source and enabled to retain said information during power-on conditions;
6 processing circuitry coupled to said volatile memory to process
7 said information during said periods of activity; and
8 a volatile memory checker enabled to execute between said
9 periods of activity, said volatile memory checker including test code
10 configured to detect errors within said information retained in said volatile
11 memory.
- 1 2. The system of claim 1 wherein said volatile memory, said processing
2 circuitry and said volatile memory checker are integrated into a single
3 integrated circuit chip, said test code being configured to detect soft errors.
- 1 3. The system of claim 2 wherein said volatile memory is one or both of
2 dynamic random access memory (DRAM) and static random access memory
3 (SRAM) embedded within said integrated circuit chip, said processing circuitry
4 including a processing unit.
- 1 4. The system of claim 1 wherein said volatile memory checker includes a
2 timing module enabled to trigger execution of said test code in response to
3 detection of a passage of a preselected time period and simultaneous
4 detection that said device is in a period of inactivity.
- 1 5. The system of claim 1 further comprising a recovery module responsive
2 to said volatile memory checker to selectively trigger information replacement
3 for said volatile memory upon detecting said errors, said information being
4 executable code for operating said device.

ELECTRONICALLY FILED

1 6. The system of claim 5 wherein said recovery module is configured to
2 selectively reinitialize said device to initiate a transfer of said executable code
3 from said source to said volatile memory.

1 7. The system of claim 5 wherein said recovery module is configured to
2 selectively reset said device in response to a system-wide error in execution
3 of said executable code.

1 8. The system of claim 5 wherein said volatile memory checker is configured
2 to perform a cyclic redundancy check (CRC) or checksum of executable code
3 memory space of said volatile memory.

1 9. The system of claim 1 wherein said volatile memory, said processing
2 circuitry and said volatile memory checker are integrated into an application
3 specific integrated circuit (ASIC) of a printer controller.

1 10. The system of claim 1 wherein said volatile memory and said processing
2 circuitry are housed within separate integrated circuit chips.

1 11. A method of assessing integrity of executable code comprising the
2 steps of:
3 transferring said executable code into volatile memory of a
4 device that is activated upon execution of said executable code, said device
5 being in an inactive state between executions of said executable code;
6 performing time-based volatile memory checking routines in
7 response to detecting that said device is in said inactive state and a
8 preselected time period has elapsed, including checking code space of said
9 volatile memory to detect errors within said executable code; and
10 initiating a selected response upon detecting fatal code error
11 during performing said checking routines.

1 12. The method of claim 11 wherein said step of performing said routines
2 includes calculating a cyclic redundancy check (CRC) or checksum for
3 executable code space of said volatile memory.

1 13. The method of claim 11 wherein said step of initiating said selected
2 response includes triggering a reinitialization that repeats said step of
3 transferring said executable code into said volatile memory.

1 14. The method of claim 13 wherein said step of initiating further includes
2 resetting said device in response to a code error that results in said checking
3 routines being terminated.

1 15. The method of claim 11 wherein said step of transferring includes loading
2 said executable code into random access memory embedded in an integrated
3 circuit having a central processor.

1 16. The method of claim 15 wherein said step of performing said checking
2 routines includes scheduling said checking routines to occur on a periodic
3 basis.

1 17. An integrated circuit comprising:
2 a processor;
3 embedded volatile memory having an input to receive
4 executable code that includes instructions specific to operations of said
5 processor;
6 an integrated self-tester having stored test code specific to
7 detecting code error in said executable code during storage in said volatile
8 memory, said self-tester being responsive to a time-based test initialization
9 signal for triggering periodic testing; and
10 a recovery module responsive to said self-tester to induce an
11 operational sequence that transfers fresh executable code to said input of
12 said volatile memory when said self-tester detects a specific code error
13 condition.

1 18. The integrated circuit of claim 17 wherein said volatile memory is one or
2 both of dynamic random access memory (DRAM) and static random access
3 memory (SRAM), said specific code error condition including alpha particle-
4 induced error detections that are pre-identified as being fault conditions.

1 19. The integrated circuit of claim 17 wherein said self-tester includes
2 embedded non-volatile memory for storing said test code.

1 20. The integrated circuit of claim 17 wherein said processor and said
2 executable code are specific to operating within a printer controller.

1 21. The integrated circuit of claim 17 wherein said recovery module includes
2 code for inducing reinitialization in which said volatile memory is reloaded with
3 said executable code from a source of said executable code.

1 22. A system for managing information storage comprising the steps of:
2 storing said information within memory that is susceptible to
3 occurrences of soft errors, said memory being within a device that is
4 characterized by extended periods of inactivity between periods of activity;
5 processing circuitry coupled to said memory to process said
6 information during said periods of activity; and
7 an automated memory checker enabled to execute between
8 said periods of activity, said automated memory checker being configured to
9 execute test code on a timed basis to detect said soft errors within said
10 information stored in said memory.

1 23. The system of claim 22 wherein storing said information in memory
2 includes magnetically recording said information on a medium susceptible to
3 said occurrences of soft errors.

20070424

- 1 24. The system of claim 22 wherein storing said information includes
- 2 embedding said information within non-volatile memory housed within an
- 3 integrated circuit chip, wherein said non-volatile memory is susceptible to said
- 4 occurrences of soft errors.

2007-10-24 14:00:00